UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/559,876	12/07/2005	Huafeng Dai	L4050.0006	2854

32172 7590 10/15/2008

DICKSTEIN SHAPIRO LLP
1177 AVENUE OF THE AMERICAS (6TH AVENUE)
NEW YORK, NY 10036-2714

EXAMINER	
KING, JOHN B	

ART UNIT	PAPER NUMBER
4148	

MAIL DATE	DELIVERY MODE
10/15/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/559,876	DAI ET AL.	
	Examiner	Art Unit	
	JOHN B. KING	4148	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 December 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 December 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *12-7-2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The instant application having Application No. 10559876 filed on December 7, 2005 is presented for examination by the examiner.

Oath/Declaration

2. The applicant's oath/declaration has been reviewed by the examiner and is found to conform to the requirements prescribed in **37 C.F.R. 1.63.**

Priority

3. As required by **M.P.E.P. 201.14(c)**, acknowledgement is made of applicant's claim for priority based on applications filed on June 13, 2003 (CHINA 03137109.4).

Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Drawings

4. The applicant's drawings submitted are acceptable for examination purposes.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 1 and 10 are rejected under 35 U.S.C. 102(b) as being anticipated by Shumueli et al. (US 2002/0147912 A1) published October 10, 2002, hereinafter referred to as Shumueli.

As per **claim 1**, Shumueli discloses an authentication method based on private bytes of USB flash memory media **[portable memory device]**, comprising **(paragraphs 6 and 41, Shumueli teaches having a portable memory device. In the absent of any new or unexpected results, the portable memory device of Shumueli is considered similar to the applicant's USB flash memory media. In paragraph 8, Shumueli also discloses that the information stored on the portable memory device is encrypted and therefore private to anyone except the authorized user.)**: step 10, reading authentication information from the private bytes of the USB flash memory media by an authentication unit **[host] (paragraph 9, Shumueli teaches comparing authentication information from the portable memory device to the authentication information that the user has entered.)**; step 20, authenticating, by the authentication unit, the authentication information input by a user by using the authentication information read from the private bytes of the USB flash memory media **(paragraphs 35-36, Shumueli teaches the user inputting authentication information and the authentication routine comparing the user information to the authentication information stored on the portable memory device.)**; step 30, determining whether the authentication is successful or not, if it is

successful, opening an operation authorization **[keylet]** based on the authentication information, otherwise, executing a process for failed authentication **(paragraph 36, Shumueli teaches that if the user is authenticated another keylet (program) is performed based upon user preferences. Shumueli also teaches that if the user is not authenticated that the authentication routine will either ask the user to re-enter the authentication information or end the process.)**

As per **claim 10**, Shumueli discloses the authentication method based on private bytes of USB flash memory media according to claim 1 **[See rejection to claim 1 above]**, wherein a control chip **[control circuitry]** of the USB flash memory media receives a read/write instruction sent from the authentication unit **(paragraph 25, Shumueli teaches that the key (portable memory device) contains control circuitry to interact with the host and perform data organization. One part of data organization includes the reading and writing of data.)**, determines whether a read/write operation is executed to the private bytes, if it is, the read/write operation to the private bytes is executed, if it is not, the read/write operation to normal bytes is executed **(paragraphs 75-76, Shumueli teaches the encryption/decryption of the data on the portable memory device. Shumueli also discloses users having read/write permissions and different security levels. It is inherent that different security levels can include encryption if the data needs a higher level of security. In order for the encryption to occur there has to be some signal to determine if the data needs to be encrypted or not.)**

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 2-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shumueli in view of James (US 20030212862 A1), filed March 12, 2003.

As per **claim 2**, Shumueli discloses the authentication method based on private bytes of USB flash memory media according to claim 1 **[See rejection to claim 1 above]**, wherein before the step 10, further comprising: step 1, detecting whether the USB flash memory disk is connected to the authentication unit **(paragraph 33, Shumueli teaches that the process begins when the key (portable memory device) is inserted into the host. Therefore, the portable memory device has to be connected to the host before the authentication routine can be executed.)**, if it is, executing the step 10; step 2, inquiring the user whether to re-authenticate or not **(paragraph 36, Shumueli teaches that the user may try to re-enter the authentication information if the first authentication failed, or the user can end the process.)**, Shumueli also discloses determining that the authentication is failed, and executing the process for failed authentication **(paragraph 36, Shumueli teaches that after authentication has failed the authentication routine will either end the process or ask the user to re-enter the authentication information.)**

However, Shumueli does not disclose asking the user to connect the USB flash memory to a USB interface to re-authenticate.

James discloses prompting the user to connect a USB flash memory media **[memory device]** to an USB interface **(paragraphs 27-28, James teaches prompting the user to reconnect the memory device to the host if it becomes disconnected in order to complete a predetermined task. The process of re-authentication is a predetermined task.)**

Shumueli and James are analogous art because they are from the same field of endeavor of using a memory device to perform user authentication.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the portable memory device to perform user authentication as taught by Shumueli by adding allowing the user to reconnect the device if needed as taught by James because this would improve data integrity in the case of an accidental disconnection **(James, paragraph 12, discloses some advantages of having improved data integrity during "surprise" disconnections.)**

As per **claim 3**, Shumueli in view of James discloses the authentication method based on private bytes of USB flash memory media according to claim 2 **[See rejection to claim 2 above]**, wherein the process for failed authentication in the step 30 is to execute the step 2 **(paragraph 36, Shumueli teaches having the user re-enter the authentication information if the authentication routine returned that the previous authentication failed.)**

As per **claim 4**, Shumueli discloses the authentication method based on private bytes of USB flash memory media according to claim 1 **[See rejection to claim 1 above]**, wherein before the step 10, further comprising: step 1', detecting, by the authentication unit, whether the USB flash memory disk is connected to the authentication unit or not **(paragraph 33, Shumueli teaches that the process begins when the key (portable memory device) is inserted into the host. Therefore, the portable memory device has to be connected to the host before the authentication routine can be executed.)**;

Shumueli also discloses step 5', if the connection is held, then executing the step 10 **(paragraph 9, Shumueli teaches comparing authentication information from the portable memory device to the authentication information that the user has entered. In order to read the authentication information from the portable memory device the device has to stay connected.)**; otherwise, executing the step 3' **(paragraphs 27-28, James teaches prompting the user to reconnect the memory device to the host if it becomes disconnected in order to complete a predetermined task. The process of re-authentication is a predetermined task. Shumueli, paragraph 9, also teaches the authentication process.)**

However, Shumueli does not teach checking the connection again or prompting the user to re-connect the USB flash memory device.

James discloses the step 2', if the connection is held, executing the step 1' after a predetermined time period, and if the connection is not held, then locking the operating system **(paragraph 27, James teaches monitoring the connection and**

disconnection of memory devices. One way to check to see if the memory device has been disconnected is to keep checking the connection again after a certain period of time has passed. James also teaches having certain connection or disconnection events occur after a connection or disconnection. James discloses a memory device that allows for security and access control, so it would be obvious for a disconnection event to lock the operating system to prevent unauthorized access to the system.); step 3', prompting the user to connect the USB flash memory media **[memory device]** to the USB interface and inputting the authentication information **(paragraphs 27-28, James teaches prompting the user to reconnect the memory device to the host if it becomes disconnected in order to complete a predetermined task. The process of re-authentication can be considered a predetermined task. Shumueli, paragraph 9, also teaches the authentication process.)**; step 4', detecting, by the authentication unit, whether the USB flash memory media is connected to the authentication unit **(paragraph 27, James teaches monitoring the connections and disconnections of the memory devices.)**;

Shumueli and James are analogous art because they are from the same field of endeavor of using a memory device to perform user authentication.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the portable memory device to perform user authentication as taught by Shumueli by adding monitoring for disconnections as taught by James because this would allow for improved data integrity in case of an accidental disconnection **(James,**

paragraph 12, discloses some advantages of having improved data integrity during "surprise" disconnections.)

As per **claim 5**, Shumueli in view of James discloses the authentication method based on private bytes of USB flash memory media according to claim 4 **[See rejection to claim 4 above]**, wherein the process for failed authentication in the step 30 is to release the lock of the operating system and execute the step 1' if it is successful, otherwise, execute the step 4' **(James, paragraph 27, teaches the process of determining if the memory device is connected or not and performing certain events based upon if the device is connected or not, such as locking the operating system. Shumueli, paragraph 9, teaches the process of user authentication through the portable memory device. It would have been obvious to one of ordinary skill in the art at the time of the invention to know that in order for the user to attempt to re-authenticate, the operating system must be unlocked to allow the user to enter their authentication information.)**

9. Claims 6 and 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shumueli in view of King et al. (US 20020044663 A1), published April 18, 2002, hereinafter referred to as King.

As per **claim 6**, Shumueli discloses the authentication method based on private bytes of USB flash memory media according to claim 1 **[See rejection to claim 1 above]**, further comprising the step of setting the authentication information to the private bytes of the USB flash memory media when the authentication unit is installed

(paragraphs 81-84, Shumueli teaches the initialization of the user authentication on the portable memory device.), the setting step comprising: step A, sending the authentication information input by the user to the private bytes of the USB flash memory media by the authentication unit **(paragraphs 81-84, Shumueli teaches the initialization of the user authentication on the portable memory device. In order to initialize the user authentication information, it is inherent that the user must input the information. It is also inherent that the user authentication information has to be stored somewhere for it to be able to be used at a later time. Shumueli, Figure 1, teaches the portable memory device having an area of memory that would allow for the storing of the user authentication information. In paragraph 8, Shumueli also teaches that most of the stored data should be encrypted to enhance security and will therefore be private to most users of the memory device.)**;

However, Shumueli does not disclose determining if the write operation was successful or not.

King discloses step B, determining whether the operation of writing the authentication information into the private bytes of the USB flash memory media is successful **(Figure 10, King teaches checking to see if a memory write to a smart card is successful or not.)**, if it is successful, opening an operation authorization based on the authentication information, otherwise, executing a subsequent process for failed authentication if the operation of writing the authentication information is not successful **(Figure 10, King also teaches that if the memory write is successful a**

certain action is performed and if the memory write is not successful a different action is performed. Shumueli, paragraphs 35-36, teaches performing the user authentication which executes a particular program if the user is not authenticated.)

Shumueli and King are analogous art because they are from the same field of endeavor of using a memory device for security purposes.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the portable memory device to perform user authentication as taught by Shumueli by adding determining if the memory write of the user authentication information was successful as taught by King because this would allow for better data integrity in the security system.

As per **claim 7**, Shumueli in view of King discloses the authentication method based on private bytes of USB flash memory media according to claim 6 **[See rejection to claim 6 above]**, wherein the operating system log-on information of the user is contained in the authentication information **(paragraph 35, Shumueli teaches that in order to authenticate a user, the user may enter logon information.)**

10. Claims 8, 9 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shumueli in view of King et al. (US 20020044663 A1), published April 18, 2002, hereinafter referred to as King and further in view of James.

As per **claim 8**, Shumueli in view of King discloses the authentication method based on private bytes of USB flash memory media according to claim 6 or 7 **[See**

rejection to claim 6-7 above], wherein before the step A, further comprising: step X, detecting, by the authentication unit, whether the USB flash memory disk is connected with the authentication unit, if the connection is held, executing the step A **(paragraphs 81-84, Shumueli teaches the initialization of the user authentication on the portable memory device. In order to initialize the user authentication information, the portable memory device must be connected to the host.)**; Shumueli also teaches ending the setting process if the authentication has failed.

However, Shumueli in view of King does not disclose prompting the user to re-connect the memory device.

James discloses step Y, inquiring the user whether to re-authenticate or not, if the user determines to re-authenticate, then prompting the user to connect the USB flash memory disk to the USB interface **(paragraphs 27-28, James teaches prompting the user to reconnect the memory device to the host if it becomes disconnected in order to complete a predetermined task.)**, and executing the step X after confirming the connection **(paragraph 27, James teaches monitoring the connection and disconnection of memory devices. James also teaches having certain connection or disconnection events occur after a connection or disconnection. Shumueli, paragraph 33, also teaches that the authentication process begins when the key (portable memory device) is inserted into the host.)**; otherwise, determining that the authentication is failed, and ending the setting process **(paragraph 35, Shumueli teaches that if the user authentication is not successful that the authentication routine can end the process.)**

Shumueli and James are analogous art because they are from the same field of endeavor of using a memory device to perform user authentication.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the portable memory device to perform user authentication as taught by Shumueli by adding monitoring for disconnections as taught by James because this would allow for improved data integrity in case of an accidental disconnection **(James, paragraph 12, discloses some advantages of having improved data integrity during "surprise" disconnections.)**

As per **claim 9**, Shumueli in view of King and further in view of James discloses the authentication method based on private bytes of USB flash memory media according to claim 8 **[See rejection to claim 8 above]**, wherein the subsequent process for failed authentication in the step B is to execute the step Y **(Shumueli, paragraph 36, teaches that if the user authentication failed that the user may choose to try and re-authenticate. James, paragraph 27, discloses the re-connection of the memory device if needed.)**

As per **claim 11**, Shumueli in view of King discloses the authentication method based on private bytes of USB flash memory media according to claim 6 or 7 **[See rejection to claim 6-7 above]**, wherein before the step A, further comprising: step X, detecting, by the authentication unit, whether the USB flash memory disk is connected with the authentication unit, if the connection is held, executing the step A **(paragraphs 81-84, Shumueli teaches the initialization of the user authentication on the portable memory device. In order to initialize the user authentication information,**

the portable memory device must be connected to the host.); Shumueli also teaches ending the setting process if the authentication has failed.

However, Shumueli in view of King does not disclose prompting the user to re-connect the memory device.

James discloses step Y, inquiring the user whether to re-authenticate or not, if the user determines to re-authenticate, then prompting the user to connect the USB flash memory disk to the USB interface **(paragraphs 27-28, James teaches prompting the user to reconnect the memory device to the host if it becomes disconnected in order to complete a predetermined task.)**, and executing the step X after confirming the connection **(paragraph 27, James teaches monitoring the connection and disconnection of memory devices. James also teaches having certain connection or disconnection events occur after a connection or disconnection. Shumueli, paragraph 33, also teaches that the authentication process begins when the key (portable memory device) is inserted into the host.)**; otherwise, determining that the authentication is failed, and ending the setting process **(paragraph 35, Shumueli teaches that if the user authentication is not successful that the authentication routine can end the process.)**

Shumueli and James are analogous art because they are from the same field of endeavor of using a memory device to perform user authentication.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the portable memory device to perform user authentication as taught by Shumueli by adding monitoring for disconnections as taught by James because this

would allow for improved data integrity in case of an accidental disconnection **(James, paragraph 12, discloses some advantages of having improved data integrity during "surprise" disconnections.)**

Conclusion

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to JOHN B. KING whose telephone number is (571)270-7310. The examiner can normally be reached on Mon. - Thur. 7:30 AM - 5:00 PM est..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Thomas Pham can be reached on (571)272-3689. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JBK

/Thomas K Pham/
Supervisory Patent Examiner, Art Unit 4148